UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. STEVE WAITHE, Defendant.	Case No. 21-cr-10342-PBS

GOVERNMENT'S SENTENCING MEMORANDUM

"I know the topless thing is hard to overcome for a lot of women but these pictures are only seen by me … I hope now that I have shared pictures of myself you now feel comfortable."

"I wanted to know if you had any sort of pictures from before that were either you in a bathing suit or topless or naked etc that I can compare? I know that's aggressive lol but you are one of my best participants to date … Also I wanted to know, for the next time you take pictures, if you could do some different poses for me?"

"And don't be shy haha show as much as you can. Like I said last time I know it's uncomfortable but try to go topless if you can … Remember these pictures are strictly for analysis and are deleted immediately!"

- Steve Waithe, posing as a female researcher named "Katie" as part of his scheme to trick victims into sending him explicit photos

To many of the victims in this case, Steve Waithe presented himself as a relatable coach and mentor. To other victims, he was a work colleague or a random acquaintance. To still others, he was considered a childhood friend. However, by the time of his arrest in April 2021, Steve Waithe was to all of these women only one thing: a predator set on exploiting his position and relationships for his own pleasure and as currency in online transactions with like-minded men who find excitement and gratification from explicit photos and videos that were stolen,

"leaked," or otherwise obtained through deception. And to Waithe, these women whose trust he so readily betrayed were also only one thing: targets for exploitation and sextortion.[1]

Starting in February 2020, Steve Waithe embarked on a series of schemes designed either to dupe women into sending him explicit photos of themselves, or to flat-out steal the photos altogether. Starting with female track and field athletes at Northeastern University where he was then a coach, Waithe focused on women as young as college freshmen, taking their phones under the pretense of "filming their form" at practices and meets but in reality mining the devices for photos that interested him. Until the day of his arrest in April 2021, Waithe methodically targeted women he had known from virtually every stage of life – from childhood through college through work – and attempted to trick them into sending him explicit photos.

Waithe has left behind a devastating path riddled with literally dozens of victims whose most private and personal images were taken from them, used for Waithe's own sexual benefit, and distributed to untold creeps around the world via marketplaces designed for the trafficking of so-called "leaked" photos and videos. Given the almost incomprehensible scope and depth of his conduct, this defendant warrants a sentence that includes a period of incarceration commensurate with the damage he has done – that is, a sentence well above the Guidelines range – and to deter him and others from engaging in this kind of repugnant criminal behavior ever again. Put simply, if ever there was a defendant deserving of a substantial upward variance or departure from the Guidelines, Steve Waithe is it.

For the reasons outlined below and to be articulated at the sentencing hearing in this case, the government respectfully submits that a sentence of 84 months of incarceration, 36 months of supervised release, and a mandatory special assessment of $100 per count, along with the Special

[1] "Sextortion" is conduct designed to trick someone into providing nude images or videos, with requests for money or more images with the underlying threat that compromising images could be shared or made public if the victim does not comply with the demands. The FBI has observed a substantial increase in this type of conduct and views sextortion as a "growing threat," particularly among younger victims. *See, e.g.*, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/sextortion.

Conditions described below, is appropriate in this case and for this defendant. Such a sentence would be sufficient, but absolutely not greater than necessary, to satisfy the sentencing objectives enumerated in 18 U.S.C. § 3553(a).

FACTUAL BACKGROUND

The roots of Steve Waithe's appalling criminal conduct date back to at least 2018, when he took the first steps in a series of schemes in which he attempted, at times unsuccessfully and at times with great success, to steal explicit photos of young women and trick young women into sending photos to him under false pretenses. As a track and field coach at Northeastern University in 2018 and 2019, Waithe requested the cell phones of female student-athletes on the team under the pretense of filming them at practice and meets – that is, in his role as a trusted coach and mentor and for the stated purpose of athletic development for the young women. PSR ¶¶ 12-13. Instead of, or in addition to, filming them, Waithe scrolled through the young women's cell phones, located photos he was interested in, and covertly sent them to himself via the "direct message" feature in Instagram. PSR ¶ 13. To conceal his conduct, he then deleted the "Sent Items" from the victims' Instagram accounts. *Id*.

The Instagram Wire Fraud Scheme

Approximately a year later, and after he no longer worked at Northeastern, Waithe began registering dummy or anonymized Instagram accounts with usernames like "anon.4887" and "privacyprotecter". PSR ¶ 14. Using these accounts, he contacted prospective victims, including some of the same student-athletes from the Northeastern track and field team, and claimed that he was a "Good Samaritan" who had randomly "found" explicit photos of the female victims on the internet. *Id*. Using the dummy Instagram accounts and identifying himself at times as a woman named "Katie," he then sent victims compromising photos of themselves, including some of the photos he had stolen from their phones over a year earlier at practices and meets. PSR ¶ 15. Waithe then attempted to extort the victims for additional photos by telling them that he could help them remove the photos from the internet by conducting a "reverse image search" and

that the best solution would be for the young women to send him any additional explicit photos they might have. *Id*.

In one message, referring to the website where he had allegedly "found" the compromising photos of a victim, Waithe said, "This sick website post[s] pictures of girls without their knowledge every single day. Its thousands and thousands of girls." When asked why he was trying to "help" victims, Waithe responded, "Well the way I look at it is if I'm helping one person then I'm making the world a better place." In messages to some victims, Waithe went so far as to claim that he was working with law enforcement to apprehend the culprit who allegedly had "leaked" victims' photos: "I thought I mentioned before I am work[ing] with authorities. And that I work specifically in cyber crimes." When one victim suspected the anonymous Instagram user was actually Waithe and suggested as much, Waithe replied, "We are looking into him now. From what we are seeing it does not look like the IP address is coming from him but I want to be sure … The ip address does not match so it is not him. Still searching for who could have hacked into the university network."

Notably, none of the Northeastern student-athletes were tricked by this scheme, though Waithe continued to try it on new prospective victims, ultimately finding success with at least one.

Cyberstalking

Without immediate success from the "Instagram scheme," Waithe pursued certain victims more aggressively, ultimately crossing the line into cyberstalking. For example, from June 2020 through October 2020, Waithe cyberstalked the victim identified in the indictment as Victim 6 by: sending messages and stolen or otherwise-compromised nude photos depicting Victim 6 via Instagram, conspiring to obtain unauthorized access to her Snapchat account, stealing private photos contained in her Snapchat account, sending the private photos via Instagram to Victim 6's boyfriend, and sending additional text messages to Victim 6 from an anonymous phone number. PSR ¶ 26.

More specifically, starting one night in June 2020, at approximately 12:34 AM, Waithe began messaging Victim 6 from his "privacyprotecter" Instagram account. PSR ¶ 26. In Instagram direct messages, Waithe ultimately sent seven nude or semi-nude photos depicting both Victim 6 and another victim to Victim 6. By October 2020, Waithe had successfully orchestrated the hacking of Victim 6's Snapchat account (see below) and, using a different dummy Instagram account with the username "pvcyprotect", sent a message to Victim 6's boyfriend, stating, "I wanted to make you aware that someone hacked your girlfriend's snapchat account and will leak it soon. I need your help to assure this does not happen." *Id*. Waithe also messaged Victim 6 herself, sending photos stolen from her Snapchat account and saying, "Do these look familiar?" and "Please let me know asap". *Id*. Utilizing an app that allows users to place calls or send messages from otherwise-anonymous phone numbers, Waithe also sent text messages to Victim 6 containing stolen compromising photos and the text, "Is this you?" *Id*.

The Snapchat Hacking Computer Fraud Scheme

No later than May 2020, Waithe embarked on a new scheme to conspire with others on the internet to hack into the Snapchat accounts of young women, including multiple women he had already victimized on Instagram. To effectuate this scheme, Waithe conducted his own extensive online research in an effort to figure out how to hack into a Snapchat account which, among other things, enables users to save and store photos and videos within the app. *See* PSR ¶ 23. For example, in May 2020, Waithe conducted Google searches for "how to hack Snapchat with a username and phone number" and visited webpages entitled, "How to Hack Someones Snapchat the Easy Way" and "How to Hack Someones Snapchat Account Password Online." *Id*. That month, he also posted on, among other places, a website called "LeakedBB.com", which is designed for the sharing of stolen or "leaked" images, requesting information on "How to hack Snapchat." *Id*.

By October 2020, Waithe had communicated with the individual identified in the indictment as CC-1 about hacking into specific Snapchat accounts. PSR ¶ 24. More specifically, Waithe located and contacted CC-1 via the "LeakedBB" website, engaging him to

assist in hacking victims' accounts. *Id*. Waithe sent CC-1 the usernames and phone numbers of no fewer than 15 prospective victims, directing CC-1 to hack into the accounts and collect any images stored in them. *Id*. As a result of Waithe's direction, CC-1 successfully obtained access to Victim 6's Snapchat account and sent Waithe a link to a cloud storage folder containing photos that had been stolen from the account. *Id*. When notified of the successful hack, Waithe messaged CC-1, "Hell yeah man keep it coming I'll pay you gladly. How do you accept money?" *Id*. On October 3, 2020, Waithe sent a payment to CC-1 via Google Pay in exchange for CC-1's work in furtherance of the conspiracy. PSR ¶ 25.

In the end, Waithe conspired with CC-1 and four other individuals to attempt to hack into no fewer than 68 women's Snapchat accounts, resulting in over a dozen "successful" hacks involving the theft of images or videos of victims. From May 2020 through March 2021, Waithe posted or messaged others regarding Snapchat hacks on at least 164 individual occasions.

The Body Development Wire Fraud Scheme

Finally, in furtherance of his scheme to dupe young women into sending explicit photos to him, in March 2020, Waithe created and began utilizing Google email addresses in the names of "Katie Janovich" and "Kathryn Svoboda." PSR ¶ 18. For over a year, Waithe used these email addresses – and these fake female personas – to trick young women into thinking that he was a female researcher examining "body development," with a focus on women who had competed in collegiate athletics and who were making the transition to post-college and post-competition life. For many victims, Waithe told women he knew in real life about a "friend of his" who was conducting this research and offered to put victims in touch with "her." Then, Waithe pretended to be "Katie" or "Kathryn" and emailed these prospective victims, explaining in detail the so-called "body development research" and soliciting nude or semi-nude photographs in order to "track their progress" during the course of the "study." *Id*.

Waithe's emails – from the "Katie Janovich" or "Kathryn Svoboda" email accounts – contained an introduction like, "My name is Katie, Steve told me to reach out to you in hopes for you to help us with our research!" PSR ¶ 19. The emails described the phony study and request

information relating to height, weight, body fat, and diet habits. Waithe then included what he called the "most important" request – that is, for the victims to send photos of themselves in a "uniform or bathing suit to show as much skin as possible." PSR ¶ 20. In the emails, Waithe explained, "Most women have just sent a bunch of pictures in a bra and a thong because it shows the most. Regular deep cut bras are best if you want to go topless that's best women have done that too because the easiest places the body usually shows changes is the butt and the breasts." *Id*. In the emails, Waithe provided the "reassurance" that the victims' photos would not be shared or saved. In one or more emails, Waithe wrote, "DISCLAIMER: My research is protected by HIPAA … The information is 100% confidential and your name, images, and likelihood (sic) are not included. It's strictly the data that is used in this research."

To further his efforts to persuade prospective victims to send images, Waithe concluded multiple emails with the sender ("Katie") stating that she would attach some example photos of herself and offered to send some victims a gift card upon completion of the study. *Id*. The emails included attachments of nude and semi-nude images purporting to be "Katie" but depicting yet another victim of Waithe's conduct.

In total, Waithe targeted no fewer than 62 women in the course of the "body development scheme" and successfully obtained over 400 total photos from at least 36 different victims.

Waithe's Distribution of Victims' Images

Beyond his own sexual gratification, Waithe found use for the images he had stolen from victims on the "LeakedBB" website, similar sites, the Kik messaging app, and other places, where stolen or so-called "leaked" images are points of personal pride, as well as a sort of currency among individuals who find similar gratification in such material. Sites like "LeakedBB" enable users to, among other things, communicate with one other, post publicly, and exchange links to cloud-based storage folders, frequently containing purportedly stolen or leaked images, or photos and videos otherwise obtained through deception. In these online forums, Waithe interacted with other users to distribute the explicit images he had illicitly obtained, including to trade "sets" of images with other users. In one post on the "LeakedBB"

website, Waithe wrote, "Does anyone want to trade nudes? I'm talking girls you actually know. Could be exes or hacks or whatever. I have quite a few and down to trade over snap or something." In another post, he wrote, "I'm looking for someone to trade with. Not stuff from here. Girls you may know. Hacks. Or exes. I have a lot of good ones mostly white girls in their 20s. Send me a message if interested!"

From 2019 through 2021, Waithe posted or otherwise offered to trade images of victims no fewer than 55 times and ultimately distributed nude and/or semi-nude photos of at least 11 different victims.

DISCUSSION

I. Sentencing Guidelines Calculation

As a preliminary matter, the government agrees with most of the U.S. Probation Office's ("Probation") calculation of the Guidelines Sentencing Range ("GSR") as set forth in the final Presentence Investigation Report ("PSR"). The government agrees with Probation's application of the following enhancements:

- USSG § 2B1.1(b)(2)(A) (offense involved 10 or more victims) (Count Group 1),
- USSG § 2B1.1(b)(10)(C) (sophisticated means) (Group 1),
- USSG § 2B1.1(b)(18) (violation of 18 U.S.C. § 1030 with intent to obtain and disseminate personal information) (Group 1),
- USSG § 3B1.3 (abuse of a position of trust) (Groups 1 and 2), and
- USSG § 2A6.2(b)(1)(E) (offense included pattern of activity involving stalking, threatening, or harassing same victim) (Group 2).

As calculated by Probation, the defendant's Combined Adjusted Offense Level is 23 and, with acceptance of responsibility and zero criminal history points, the resulting Total Offense Level would be 18, with a GSR of 27 to 33 months. PSR ¶¶ 34-58, 62-63, 101. The government submits, however, that one additional enhancement should apply, for Waithe's role as an organizer, leader, and/or supervisor of the criminal conduct pursuant to USSG § 3B1.1(c). PSR

at 27. Application of this enhancement would result in a one-level increase in the Combined Adjusted Offense Level and disqualify the defendant from receiving a two-level reduction for being a "zero-point offender." Waithe's resulting GSR would then be 37-46 months.

To that end, USSG § 3B1.1(c) provides for a two-level increase where "the defendant was an organizer, leader, manager, or supervisor in any criminal activity." According to one of the relevant application notes, factors to be considered when evaluating a defendant's role in criminal activity include "the exercise of decision making authority, the nature of participation in the commission of the offense, the recruitment of accomplices[,] and the degree of control and authority exercised over others." USSG § 3B1.1, App. Note 1. Here, Waithe initiated contact with CC-1 to enlist his assistance in hacking into victims' Snapchat accounts, provided CC-1 with the Snapchat usernames and corresponding phone numbers for at least 15 different prospective victims, directed CC-1 to hack into the victim's accounts, and ultimately made payments to CC-1 in exchange for CC-1's assistance in hacking the accounts and stealing victims' private photos. Later, Waithe sent photos obtained through the Snapchat hack to Victim 6 and Victim 6's boyfriend, in furtherance of his attempts to defraud and cyberstalk her. Put plainly, without Waithe's organization of the criminal conduct and his direction and supervision of CC-1, none of the 15 prospective victims would have been subjected to the criminal conduct charged in Counts 14-15 of the indictment. He conceived of the conspiracy, directed all of the conduct in furtherance of the conspiracy, and reaped the benefits procured by his subordinate co-conspirator. He was the organizer, leader, and supervisor of the conspiracy and should receive the Guidelines enhancement specifically designed for his aggravating role.

II. Sentencing Recommendation

The government's recommended sentence – including 84 months of incarceration – is the reasonable and just outcome in a case where the Guidelines fail to even remotely take into account the nature, scope, and breadth of the defendant's criminal conduct. The government's recommendation is the product of an enormous amount of thought and consideration, and its request of the Court – that is, to vary or depart so substantially upwards from the GSR – is made

with the understanding that such a request is highly unusual.[2] That said, the government submits that Steve Waithe's criminal conduct, and the harm he has wrought on no fewer than 56 women, cries out for this sentence and the requisite upward variance or departure it entails.

Pursuant to 18 U.S.C. § 3553(a), the Court is required to consider a series of factors when determining an appropriate sentence. These factors include "the nature and circumstances of the offense and the history and characteristics of the defendant"; the four legitimate purposes of sentencing; "the kinds of sentences available"; the Guidelines range itself; any relevant policy statements by the Sentencing Commission; "the need to avoid unwarranted sentence disparities among defendants"; and "the need to provide restitution to any victims." 18 U.S.C. § 3553(a).

In determining the appropriate sentence, the statute directs judges to "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing. Section 3553(a) also mandates that the sentence reflect the seriousness of the offense to, among other things, promote respect for the law, provide just punishment, adequately deter criminal conduct, and protect the public from further crimes of the defendant. Here, virtually every consideration enumerated in § 3553(a) weighs in favor of a longer sentence.

A. The Nature and Circumstances of the Offense Warrant a Sentence Well Above the GSR

The crimes that Steve Waithe perpetrated against 56 women, and attempted to perpetrate against 72 more, are deeply personal, sexual, exploitative crimes that will have profound lifelong consequences for his victims. Most counts of the indictment in this case – specifically, the wire and computer fraud counts – are typically reserved for "traditional" white-collar fraud and, as such, the Sentencing Guidelines are driven in large part by pecuniary loss. *See* USSG § 2B1.1.

[2] In this section, the government styles its requested sentence as an upward variance, warranted through consideration of the Section 3553(a) factors. The government submits that the criminal conduct described herein likewise would qualify for an upward departure on the grounds described later in this memorandum. In the end, the government defers to the Court as to whether, if it agrees that an above-Guidelines sentence is warranted, to do so via variance or via departure.

Here, these statutes were utilized because, put simply, state and local criminal laws have not caught up to the type of conduct in which Waithe was engaged. To be sure, he committed every element of each charged federal crime, but the manner in which he did so defies the conventional wisdom underlying the applicable Guidelines section. As a result, the GSR as computed by Probation (27-33 months) or even when applying the government's requested leader/organizer enhancement (37-46 months) does not come close to meeting the sentencing objectives of Section 3553(a) in this case and for this defendant.

Indeed, it is impossible to overstate the impact of Waithe's conduct on so many of his dozens of victims. Mostly from behind the curtain of a computer screen, Waithe exacted truly devastating consequences on young women across the country. He purposefully targeted women he knew would be susceptible to his tactics, including college student-athletes for whom he was supposed be a coach and mentor, as well as women just a few years older whom he knew were likely to have insecurities about their bodies as they transitioned from constant athletic competition to white-collar careers. The photos that he flat-out stole and that he deceived women into sending to him are the most personal possible images anyone could have. These were photos that were taken and kept by the victims, in private, and their value rested exclusively in the victims' own control over who – if anyone else, ever – would have possession of them. Their complete loss of that control, forever, may be the worst of many profound consequences for the victims.

Waithe's victims are now nurses, teachers, dieticians, coaches, and graduate students. And they live in constant fear that they will hear from someone about explicit photos on the internet, or that as part of a grad school or job application someone will conduct the wrong Google search. As one victim recounts, "Instead of being coached that year, I was targeted, groomed, preyed on, and repeatedly violated. He stole my phone, my photos, and my right to privacy." She continues, "The pain and emotional damage I've endured over the past several years is immeasurable. It has haunted me through every new [phase] of my life, always existing like a black cloud plotting its next storm. I constantly feel violated, used, and fearful."

Another victim states, "I am a therapist. I have clients who I am meant to support and help every day, and one of the most important pieces of my work is the therapeutic relationship. I can't imagine how those relationships would be altered and quite possibly destroyed if they were ever to come across the private images that Mr. Waithe stole from me and distributed without my consent." Regarding the lifelong consequences of Waithe's conduct, another victim wrote, "I struggle to accept I will never know the true dissemination of my compromised privacy."

In light of the massive scope of Steve Waithe's criminal behavior, combined with the deeply personal and sexual nature of the conduct and the lifelong impact his crimes will have for the victims, a sentence of 84 months would provide just punishment for the impact Waithe has had on the lives of no fewer than 56 different women.

B. Specific and General Deterrence

The Court also must consider the need for the sentence to afford adequate deterrence to criminal conduct. 18 U.S.C. § 3553(a)(2)(B). Here, the Court must be concerned with both specific and general deterrence.

First, an 84-month sentence is necessary to deter Waithe from reoffending upon his release from custody. This is not a case in which the defendant committed one bad act or where he happened to be caught crossing the line on his worst day. This case did not involve a mistake or momentary lapse in judgment. Rather, it was a long series of calculated steps. Waithe was engaged for over a year in an ever-evolving set of schemes, and it required methodical work on virtually a daily basis. His internet search and browser history, combined with the dates on which he was messaging victims and posting about his conquests, betray how regularly Waithe was engaged in conduct to support and sustain his seemingly insatiable need for *more*. Time and again, Waithe researched how to disguise Instagram accounts and how to hack into Snapchat accounts; time and again, he contacted prospective victims via Instagram or email; time and again, he pretended to be a woman named "Katie" to trick victims into sending him the most private of pictures; and time and again, he communicated with co-conspirators and prospective

"trading partners" on websites and messaging apps. To further his Instagram, Snapchat, and "body development" schemes, Waithe created and maintained at least 22 different online accounts across at least seven different platforms. In total, Waithe successfully obtained over *one thousand* images of victims that he ultimately used for personal gratification, to brag about and trade with others online, and to harass and ultimately cyberstalk victims.

If the virtually constant efforts in 2020 and 2021 prior to his arrest were not enough to demonstrate the risk of Waithe's recidivism, the Court need look no further than Waithe's conduct during his period of pre-trial release. As the Court is aware, Waithe was arrested on April 7, 2021 and ultimately released on conditions, including prohibitions that he not commit further crimes and that he not access the internet outside of certain strict parameters. However, a search warrant conducted on Waithe's personal Instagram account in 2022 revealed that Waithe had been regularly and repeatedly violating the terms of his pretrial supervision by using Instagram to view photos of young women ***and to send direct messages requesting that the prospective new victims send him photographs of themselves***. PSR ¶ 28. Indeed, subsequent to his arrest in this case and in plain violation of his bail conditions, Waithe logged into his primary Instagram account on no fewer than 135 separate occasions. PSR ¶ 29.

In one conversation on Instagram in late May and early June 2022 – so, a year after his arrest – Waithe complimented a young woman via Instagram direct message and offered to pay her in exchange for allowing him to make "drawings" using photos of her. PSR ¶ 30. He wrote, "I would just need a bunch of pictures of you preferably with all of your tattoos showing because it makes for more detail in the drawings. It wouldn't be posted anywhere or anything haha. I can give it to you personally but it's for my portfolio I'm working on." *Id*. In a conversation with another prospective victim on Instagram in June 2022, Waithe told a young woman that she is in "such great shape" and offered her $50 to participate in a "study." *Id*. He then wrote, "Haha it's just you being yourself" and "Of your most confident sensual picture." *Id*. Even facing the charges in this case, Waithe demonstrated that he is willing and able to flout the

Court's restrictions and reengage in conduct that is ***virtually identical*** to that giving rise to the indictment.

Second, a significant sentence is also necessary to provide general deterrence to others similarly situated who might be tempted to engage in the same course of conduct. Online predators generally believe that because they are hiding behind their computers, the government is less likely to detect and prosecute them if they commit an offense. The ability to operate anonymously with relative ease may cause them to believe – mistakenly – that they are not committing a serious offense – or, because they are not committing a "hands-on" offense, they can get away without severe penalty. When law enforcement is able to unwind a network of aliases and anonymous accounts and convict a defendant, however, it is important that a Court's sentence adequately deter others from engaging in the same conduct. If cyber criminals believe that only mild punishment will follow, there is a real risk that they will not be deterred from harming their victims. In this case, and as discussed throughout this memo, a Guidelines sentence would send exactly the wrong signal: prospective criminals can victimize women across the country like Waithe did, inflicting lifelong consequences, and face just a couple of years of imprisonment. The government submits that the Court should send the opposite message and do so with a sentence substantially above the calculated GSR.

C. Waithe's History and Characteristics

Waithe's history and characteristics also weigh in favor of a longer incarcerative sentence. *See* 18 U.S.C. § 3553(a)(1). Waithe has had more advantages than most defendants who appear before this Court. He attended Penn State University and was an All-American athlete. PSR ¶ 84. He has a loving, supportive family, including two devoted parents, as well as close siblings. PSR ¶ 69. Unlike many of the defendants who appear before this Court, Waithe has not struggled with poverty, addiction, or a lack of opportunity. To be clear, while these challenges do not excuse criminal behavior, they sometimes provide context for criminal conduct. That is not the case here. There are no mitigating factors in this case, and the defendant should be sentenced accordingly.

D. Proportionality

Given the nature of Waithe's crimes and the stark contrast between his conduct and that typically associated with more conventional white-collar fraud, there are very few comparable cases, even nationwide. To be sure, some defendants have been convicted of crimes involving the theft of photos and the compromise of social media accounts. *See, e.g.*, *United States v. Moore & Evens*, Case No. 13-cr-00917-DMG (C.D. Cal. Dec. 9, 2015) (sentences of 25-30 months for defendants who obtained and/or disseminated stolen images of victims); *United States v. Faber*, Case No. 8:21-cr-00021-MAD (N.D.N.Y. Aug. 19, 2021) (sentence of 36 months for defendant who obtained and disseminated nude photos and videos of victims); *United States v. Chi*, Case No. 8:21-cr-270-KKM-TGW (M.D. Fla. 2022) (sentence of 60 months for unauthorized access of at least 306 victim accounts). However, the conduct of the defendants in each of these cases appears to differ wildly from that of Waithe, particularly when looking at the nature of the offenses, the diversity of scope, and the defendants' relationship to victims.

Here, the government submits, while other defendants may have engaged in a single "sextortion" scheme, Waithe actually embarked on no fewer than four, evolving and honing his effectiveness as time went on. Moreover, most defendants prosecuted for "similar" conduct were accused of hacking the accounts of complete strangers, whereas Waithe targeted people with whom he had preexisting relationships. Notably, none of the "similar" cases reviewed to date also include a cyberstalking charge which, the government submits, further differentiates the instant case.

Where Waithe's conduct may differ most from "comparable" cases, however, is in the "body development scheme." To be sure, defendants in other cases were convicted for engaging in similar conduct, hacking into various online accounts the way Waithe and his co-conspirators victimized women through Snapchat. However, when Waithe embarked on his scheme with his fake female personas, Katie Janovich and Kathryn Svoboda, he crossed into uncharted territory: by introducing victims to the fake "body development study" and soliciting photos to be taken in real-time, Waithe began ***inducing*** women to create new explicit photos that he could obtain,

make personal use of, and distribute on the internet. The government submits that the depth of this deceit amplifies the victimization of the women subjected to Waithe's "body development research" conduct and, especially when taken together with the other wire fraud, computer fraud, and cyberstalking, differentiate Waithe from defendants in other cases.

E. Need to Protect the Public

Finally, a significant sentence also is appropriate pursuant to 18 U.S.C. § 3553(a)(2)(C) to protect the public from this defendant. Waithe's conduct should cause concern for literally any woman with whom he interacts. By his conduct in this case, Waithe has proven himself willing and able to try to take advantage of virtually any woman he meets. His conduct is frightening and traumatizing, and he should receive an 84-month sentence to afford the victims the knowledge that he will be unable to harm them for a lengthy period of time and to ensure that even more women are not subjected to the same type of victimization.

III. Grounds for Departure and Special Conditions

As the Court is uniquely aware, when considering a sentence above the calculated Guidelines range, the sentence can be imposed as either a variance or a departure. While the above arguments provide the government's proposed basis for a variance, four different sections of the Guidelines provide a basis in this case for an upward departure. Notably, Probation identified two of these Guidelines sections in the PSR and noted that the Court "may wish to consider" them as potential grounds for departure. PSR ¶ 116.

First, Application Note 21(A) in USSG § 2B1.1 ("Upward Departure Considerations") specifically provides a basis for "cases in which the offense level determined under this guideline substantially understates the seriousness of the offense." As discussed extensively above, this is such a case. Application Note 21(A) includes a "non-exhaustive" list of the factors that may be considered. Three of these factors describe precisely aspects of Waithe's criminal conduct:

(1) A primary objective of the offense was an aggravating, non-monetary objective – that is, personal, sexual gratification and to trade with others for additional "leaked" photos, under App. Note 21(A)(i);

(2) The offense caused or risked substantial non-monetary harm – specifically, psychological and emotional harm of victims and the non-monetary loss of the images themselves, under App. Note 21(A)(ii); and

(3) Waithe committed the computer fraud and computer fraud conspiracy to further a broader criminal purpose – that is, to use the photos stolen from hacked Snapchat accounts in an effort to further defraud victims for more photos.

Second, USSG § 5K2.0 provides a basis for upward departures where there are aggravating circumstances not otherwise taken into account or based on "circumstances of a kind not adequately taken into consideration." The Guidelines note that departures under §5K2.0 may be warranted in "an exceptional case," and the government submits for all the reasons enumerated herein, this is such a case.

Third, USSG § 5K2.9 provides for an upward departure where "the defendant committed the offense in order to facilitate or conceal the commission of another offense." Here, Waithe's wire and computer fraud schemes were designed, in no small part, to facilitate his ongoing efforts to dupe women into sending him compromising photos.

Fourth, USSG § 5K2.21 provides for an upward departure "to reflect the actual seriousness of the offense based on conduct … underlying a potential charge not pursued in the case." Here, Waithe engaged in substantial criminal conduct that was not charged in the indictment, as reflected in the victimization of dozens of women across the country for whom there were not specifically-enumerated charges in the indictment, along with additional computer fraud conspiracies.

As a final request, the government proposes four additional "Special Conditions" and asks that they be included upon imposition of the sentence: (1) no contact, direct or indirect, with any victims or attempted victims; (2) internet use only under the monitoring or supervision of Probation (if this is possible); (3) no use of any social media; and (4) no requests for photos, images, videos, or any other media from anyone.

CONCLUSION

For all of the foregoing reasons, the government respectfully recommends that the Court impose a sentence of 84 months of imprisonment, three years of supervised release, the mandatory special assessment of $100 per count, and the Special Conditions described above. Such a sentence would be sufficient, but not greater than necessary, to reflect the seriousness of the offenses and the goals of sentencing.

Respectfully Submitted,

JOSHUA S. LEVY
Acting United States Attorney

Date: March 1, 2024

By: */s/ Adam W. Deitch*
Adam W. Deitch
Assistant United States Attorney
United States Attorney's Office
One Courthouse Way
Boston, MA 02210
617-748-3123

CERTIFICATE OF SERVICE

Undersigned counsel certifies that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants.

/s/ Adam W. Deitch
Adam W. Deitch
Assistant United States Attorney

Dated: March 1, 2024